Materiał szkoleniowy dla praktykantów/ stażystów/wolontariuszy z zakresu ochrony danych osobowych

Dane osobowe

Dane osobowe – zgodnie z art. 4 ust. 1 RODO – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; w szczególności **imię i nazwisko,** PESEL**, dane o lokalizacji, identyfikator internetowy**

Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby.

Do danych takich należą informacje :

- zbierane podczas rejestracji lub podczas świadczenia usług opieki zdrowotnej,
- informacje pochodzące z badań laboratoryjnych lub lekarskich
- oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

•wyroki skazujące i naruszenia prawa

•Przynależność związkowa, polityczna, religijna, rasowa

Przetwarzanie danych osobowych

Zgodnie z RODO przez przetwarzanie danych osobowych należy rozumieć każdą czynność wykonywaną na danych osobowych a mianowicie:

- ***zbieranie,***
- ***utrwalanie,***
- ***organizowanie,***
- ***porządkowanie,***
- ***przechowywanie,***
- ***adaptowanie lub modyfikowanie danych,***
- ***pobieranie***
- ***przeglądanie,***
- ***wykorzystywanie,***
- ***ujawnianie poprzez przesłanie,***
- ***rozpowszechnianie lub innego rodzaju udostępnianie,***
- ***dopasowywanie,***
- ***łączenie,***
- ***ograniczanie,***
- ***usuwanie lub niszczenie danych.***

Polityka Bezpieczeństwa w WSP w Andrychowie

Polityka opisuje:

- reguły określające granice dopuszczalnego zachowania wszystkich użytkowników systemów,
- zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń,
- odpowiednie zabezpieczenia,
- wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych

Bezpieczeństwo **danych**

Jednym z podstawowych obowiązków Wojewódzkiego Szpitala Psychiatrycznego w Andrychowie wynikającym z RODO jest prawidłowe zabezpieczenie danych osobowych.

WSP zobowiązany jest, zgodnie z art. 32 RODO, przy uwzględnieniu różnych czynników o charakterze technicznym oraz organizacyjnym, zapewnić należyte bezpieczeństwo przetwarzanych danych.

Przykładowe środki służące zabezpieczeniu danych

- zdolność do zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie uszkodzenia fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Przykładowe środki służące zabezpieczeniu danych

- monitoring wizyjny
- kontrola dostępu
- polityka klucza
- awaryjne Źródło zasilania
- systemy przeciwpożarowy
- kopie zapasowe

Przykładowe środki służące zabezpieczeniu danych

- Bezpieczna praca z komputerem:
  - zasady pracy w systemach informatycznych regulują wewnętrzne akty prawne
  - główne zabezpieczenia to: system haseł, system antywirusowy aktualizowany na bieżąco, wylogowanie po zakończeniu pracy i odejściu od stanowiska pracy, szyfrowanie plików i dysków zawierających dane osobowe, zabezpieczenie nośników przenośnych, zabezpieczenie laptopów
  - sprzęt służbowy nie może być wykorzystywany do osobistego użytku.
  - użytkownik pracuje na własnym koncie (identyfikatorze) i HAŚLE
  - automatyczny wygaszacz ekranu

- Procedura zarządzania incydentami cyberpezpieczeństwa
- Procedura zarządzania ryzykiem w obszarze ochrony danych osobowych
- Procedura postępowania w przypadku ochrony danych osobowych

Przykładowe środki służące zabezpieczeniu danych

- Polityka czystego biurka i ekranu
- Niszczenia dokumentów zawierających dane osobowe w sposób uniemożliwiający ich ponowne odczytanie
- Niepozostawianie otwartych pomieszczeń bez nadzoru osób upoważnionych do przetwarzania danych osobowych
- Zabrania się kopiowania dokumentów zawierających całe zbiory, bazy danych i ich przenoszenie, przesyłanie poza użytkowane systemy informatyczne np. na pendriva, dodatkowe dyski przenośne, z wyłączeniem sytuacji wynikających z przepisów prawa ciążących na administratorze.

Przykładowe środki służące zabezpieczeniu danych

- Należy pamiętać, że każdy pracownik/praktykant/wolontariusz/stażysta przetwarza dane osobowe wyłącznie na polecenie administratora i w zakresie przez niego wskazanym w oparciu **o pisemne upoważnienie** do przetwarzania danych osobowych.

- W WSP w Andrychowie obowiązuje procedura nadawania upoważnień do przetwarzania danych osobowych określona w „Polityce Bezpieczeństwa w WSP w Andrychowie".

- Przetwarzanie danych osobowych przez osoby nieupoważnione jest **zabronione.**

Odpowiedzialność

- Każdy pracujący z danymi osobowymi powinien przestrzegać zasad zgodności z prawem przetwarzania danych osobowych

- Przetwarzający dane osobowe ponoszą odpowiedzialność z tytułu naruszenia obowiązujących procedur i przepisów prawa dot. ochrony danych osobowych odpowiednio do wagi naruszenia. Działania lub zaniechania powodujące naruszenie bezpieczeństwa, ochrony danych osobowych mogą skutkować m.in. nałożeniem przez administratora kary dyscyplinarnej/ porządkowej z rozwiązaniem stosunku pracy włącznie.

Poufność

- Zobowiązuję się **do zachowania w tajemnicy** wszelkich informacji o danych osobowych uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych oraz informacji o ich zabezpieczeniu.

- **Powyższej tajemnicy zobowiązuję się dochować również po zakończeniu praktyki/stażu/wolontariatu.**

- Jestem świadoma/y, że naruszenie poufności przetwarzanych danych osobowych może nieść dla mnie konsekwencje dyscyplinarne.

Poufność

- Zobowiązuję się **do zachowania w tajemnicy** wszelkich informacji o danych osobowych uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych oraz informacji o ich zabezpieczeniu.

- **Powyższej tajemnicy zobowiązuję się dochować również po zakończeniu praktyki/stażu/wolontariatu.**

- Jestem świadoma/y, że naruszenie poufności przetwarzanych danych osobowych może nieść dla mnie konsekwencje dyscyplinarne.

Kiedy ma miejsce naruszenie?

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady UE 2016/679 (RODO) **naruszenie ochrony danych osobowych to:**

„naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

- *zniszczenia, utracenia, zmodyfikowania;*
- *nieuprawnionego ujawnienia lub*
- *nieuprawnionego dostępu*

do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”.

Można wyróżnić trzy typy naruszeń ochrony danych osobowych:

NARUSZENIE POUFNOŚCI – polega na ujawnieniu danych osobowych nieuprawnionej osobie np.:

- *Przypadkowe wysłanie danych osobowych pacjenta do osoby postronnej.*
- *System informatyczny administratora został zainfekowany złośliwym oprogramowaniem. Po przeprowadzeniu wstępnej analizy administrator stwierdził, że w wyniku działania tego oprogramowania osoba nieupoważniona uzyskała dostęp do danych osobowych.*

NARUSZENIE DOSTĘPNOŚCI – polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych

- *Zgubienie lub kradzież nośnika zawierającego bazy danych klientów administratora przy braku kopii zapasowej.*
- *Pracownik przypadkowo lub osoba nieupoważniona celowo usuwa dane ze zbioru. Administrator próbuje odzyskać dane z kopii zapasowej, jednak jego działania nie przynoszą rezultatu.*
- *W wyniku przerwy w dostawie prądu lub ataku typu „odmowa usługi" (tzw. DDoS), administrator tymczasowo lub trwale traci dostęp do danych osobowych.*

NARUSZENIE INTEGRALNOŚCI – polega na zmianie treści danych osobowych w sposób nieautoryzowany.

- *Pracownik dla żartu zmienia nazwiska klientów poprzez dopisanie litery „s" na końcu każdego z nich."*

- *Z ryzykiem naruszenia praw lub wolności osób fizycznych mamy do czynienia wówczas, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono.*

Szkodami takimi są np.

- *dyskryminacja,*
- *kradzież tożsamości lub oszustwo dotyczące tożsamości,*
- *nadużycia finansowe, straty finansowe,*
- *nieuprawnione cofnięcie pseudonimizacji,*
- *utrata poufności danych osobowych chronionych tajemnicą zawodową,*
- *naruszenie dobrego imienia lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.*

- *Jeżeli naruszenie dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub danych genetycznych, dotyczących zdrowia lub życia seksualnego, należy uznać, że występuje duże prawdopodobieństwo takiej szkody.*

<u>Niemniej jednak każde z takich zdarzeń należy rozpatrywać indywidualnie.</u>

Kiedy ma miejsce naruszenie?

Przykłady naruszenia ochrony danych osobowych:

•pracownik zgubił dysk USB z danymi pacjentów;

•lekarzowi zatrudnionemu w placówce ukradziono laptopa z danymi pacjentów;

•pracownik stwierdził, że ktoś zabrał z biurka wyniki badań pacjentów;

•pracownik zauważył, że w Internecie ktoś opublikował dane osobowe pacjentów placówki;

•miał miejsce atak hakerski, wskutek którego straciliśmy dostęp do baz danych pacjentów.

Ważne: Naruszenie ma dotyczyć danych osobowych, tj. informacji o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Pracownik powinien niezwłocznie zgłosić podejrzenie naruszenia ochrony danych osobowych swojemu przełożonemu, inspektorowi ochrony danych lub bezpośrednio kierownikowi placówki. **Naruszenie jest skutkiem złamania zasad bezpieczeństwa danych**

Zgłoszenie naruszenia ochrony danych osobowych

- *Imię i nazwisko oraz informacje kontaktowe zgłaszającego*
- *Data i godzina stwierdzenia naruszenia / incydentu*
- *Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia)*
- *Jakiego systemu / aplikacji dotyczy?*
- *Na czym polega naruszenie / incydent*
- *Podjęte działania*
- *Wstępne oszacowanie szkód, jeśli doszło do takowych*
- *Komunikaty, jeśli są dostępne*
- *Podpis pracownika*
- *Data i podpis IOD*

- *(załącznik do Procedury postępowania w sytuacji naruszenia ochrony danych osobowych / Procedura reagowania na incydenty)*

Kiedy zgłaszać naruszenie urzędowi?

Administrator danych osobowych (Szpital) musi w niektórych przypadkach zgłosić naruszenie ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych (Prezes UODO). W praktyce czynności tych najczęściej dokonuje inspektor ochrony danych lub inna osoba wyznaczona przez ADO.

Jeżeli podejrzewamy wyciek danych osobowych, osoba wyznaczona przez ADO musi:

- udokumentować każde naruszenie, bez względu na jego wagę;
- ocenić, czy jest wysoce prawdopodobne, że naruszenie będzie skutkować ryzykiem naruszenia praw lub wolności osób, których dane dotyczą;
- jeżeli prawdopodobieństwo naruszenia praw lub wolności tych osób jest wysokie, należy powiadomić o naruszeniu Prezesa UODO;

Prezesa UODO powiadamiamy o naruszeniu niezwłocznie ***(nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia);***
Jeżeli od stwierdzenia naruszenia upłynęło więcej niż 72 godziny, do zgłoszenia przekazanego Prezesowi UODO, należy dołączyć wyjaśnienie przyczyn opóźnienia.

Przykłady naruszeń, w których nie wystąpiło ryzyko naruszenia praw lub wolności osób fizycznych

Przykład	Czy należy zgłosić naruszenie organowi nadzorczemu?	Czy należy zgłosić naruszenie osobie, której dane dotyczą?	Uwagi / zalecenia
Administrator przechowywał zaszyfrowaną kopię bezpieczeństwa archiwum danych osobowych na pamięci USB. Pamięć skradziono podczas włamania	**nie**	**nie**	Jeżeli dane zostały zaszyfrowane za pomocą najnowocześniejszego algorytmu, utworzono kopie bezpieczeństwa danych, unikalny klucz nie został złamany, a dane można przywrócić w odpowiednim czasie – być może naruszenie to nie podlega zgłoszeniu. Jeżeli jednak w późniejszym czasie klucz zostanie złamany, sytuacja ta będzie wymagała zgłoszenia
Krótkotrwała, kilkuminutowa awaria systemu zasilania w centrum obsługi telefonicznej administratora, w wyniku której klienci nie mogą skontaktować się z administratorem i uzyskać dostępu do swoich danych	**nie**	**nie**	Naruszenie to nie podlega zgłoszeniu, lecz mino to należy ten incydent zarejestrować na podstawie art. 33 ust. 5. Administrator musi prowadzić odpowiednie rejestry.
Szpitalna dokumentacja medyczna jest niedostępna przez 30 godzin w wyniku cyberataku.	**Tak**, szpital ma obowiązek zgłoszenia naruszenia, ponieważ może powstać wysokie ryzyko dla dobrostanu i prywatności pacjentów.	**Tak,** naruszenie należy zgłosić osobom fizycznym, na które wywiera wpływ.	
Dane osobowe znacznej liczby pracowników omyłkowo wysłano do niewłaściwej listy adresowej, na której znajduje się ponad 100 odbiorców.	**Tak**, naruszenie należy zgłosić organowi nadzorczemu	**Tak**, naruszenie należy zgłosić osobom fizycznym w zależności od zakresu i rodzaju ujawnionych danych osobowych i wagi możliwych konsekwencji	

Przykłady naruszeń, w których nie wystąpiło ryzyko naruszenia praw lub wolności osób fizycznych

Przykład	Czy należy zgłosić naruszenie organowi nadzorczemu?	Czy należy zgłosić naruszenie osobie, której dane dotyczą?	Uwagi / zalecenia
Wiadomość e-mail w ramach marketingu bezpośredniego wysłano do odbiorców w polach „do:" lub „dw:", tym samym umożliwiając każdemu odbiorcy wgląd w adresy e-mail innych odbiorców	**Tak**, zgłoszenie naruszenia organowi nadzorczemu może być obowiązkowe, jeżeli naruszenie dotyczy dużej liczby osób, jeżeli ujawniono dane wrażliwe (takie jak np. lista adresowa psychoterapeuty) lub jeżeli inne czynniki stwarzają wysokie ryzyko (np. wiadomość e-mail zawiera hasła startowe).	**Tak**, naruszenie należy zgłosić osobom fizycznym w zależności od zakresu i rodzaju ujawnionych danych osobowych i wagi możliwych konsekwencji.	Zgłoszenie może nie być konieczne, jeżeli nie ujawniono żadnych danych wrażliwych i jeżeli ujawniono tylko niewielką liczbę adresów e-mail Przy wysyłce jednej wiadomości e-mail do wielu adresatów istnieją proste środki, które pozwalają na ukrycie innych adresatów poprzez zastosowanie tzw. pola UDW nie każdy błędnie wysłany mail jest naruszeniem
Pracownik administratora porzucił dokumenty kadrowe i finansowe (zawierające m.in. takie dane, jak: imię, nazwisko, PESEL, adres zamieszkania, informacje o wynagrodzeniach) w kontenerze na odpady	**nie**	**nie**	*Jednak z uwagi na: - krótki okres jaki upłynął od zaistnienia do stwierdzenia naruszenia, - zamknięty teren zakładu pracy, - monitoring kontenerów na odpady, - podjęte natychmiastowo działania zaradcze. Mimo powagi tego zdarzenia, a w szczególności zakresu i kategorii danych,* ***prawdopodobieństwo*** *zmaterializowania się szkody dla osób, których te dane dotyczą (np. posłużenia się danymi w celu wyłudzenia ubezpieczenia)* ***ocenił jako niskie.***
Pracownik przez pomyłkę wynosi poza jej obszar teczkę z niezabezpieczonymi danymi osobowymi, wśród których znajdują się również szczególne kategorie danych osobowych. Po chwili orientuje się, że nastąpiła pomyłka i wraca zwracając teczkę. Działanie takie naruszyło zasady ochrony danych, ale nie mogło skutkować naruszeniem praw lub wolności osób fizycznych, gdyż dane nie zostały udostępnione			